IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application. No.	: 10/045,893	Confirmation No.	: 3131
1st Named Inventor	: Adusumilli	Art Unit	: 2134
Filed	: 01/12/2002	Examiner	: Brown, Christopher J.
Docket No.	: 42390.P12318X	Customer No.	: 7590

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLACEMENT SUMMARY OF CLAIMED SUBJECT MATTER SECTION OF APPEAL BRIEF

Sir:

This replacement SUMMARY OF CLAIMED SUBJECT MATTER section of the Appeal Brief is in response to the Order Returning Undocketed Appeal to Examiner mailed Dec. 17, 2009, after the filing of an Appeal Brief on December 31, 2008. Appellants respectfully request consideration of this SUMMARY OF CLAIMED SUBJECT MATTER by the Board of Patent Appeals and Interferences for the above-captioned patent application.

CERTIFICATE OF SUBMISSION/TRANSMISSION (37 CFR 1.8A)
I hereby certify that this correspondence is, on the date shown below, being:

EFS WEB
✓ *submitted electronically via EFS Web to the Patent and Trademark Office.*

FACSIMILE
☐ *transmitted by facsimile to the Patent and Trademark Office.*

Shannon Serrano 3-11-10
Shannon Serrano *Date*

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

Independent claim 33 pertains to an apparatus (e.g., security system 160 in FIG. 1; [0074]-[0078] on pgs. 22-24, security system 345 in FIG. 3; [0147]-[0149] on pgs. 47-48, security system 1312 in FIGs. 13, 14, 15, and 19; [0187] on pg. 58, security system 2300 in FIG. 23), according to a first embodiment of the invention. The apparatus is to reside in a data center ([0044]-[0047] on pgs. 10-11, e.g., data center 150 in FIG. 1; data center 340 in FIG. 3; data center 1316 in FIGs. 13, 14, 15, and 19) coupled between a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) and a server (e.g., server 390 in FIG. 3; server 1314 in FIGs. 13, 14, 15, and 19) of the data center. The apparatus comprises a first interface ([0064]-[0066] on pg. 18, e.g., network interface 350 in FIG. 3, interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to the public network to receive Secure Sockets Layer (SSL) encrypted data ([0065] on pg. 18, e.g., SSL data received on port 352 in FIG. 3; [0093] on pg. 29, block 455 in FIG. 4) from at least one wired client device (e.g., wired access device 320 in FIG. 3) and to receive Wireless Transport Layer Security (WTLS) encrypted data ([0065] on pg. 18, e.g., WTLS data received on port 354 in FIG. 3, [0089] on pg. 28, block 430 in FIG. 4) from at least one wireless client device (e.g., wireless access device 305 in FIG. 3). The apparatus also comprises client-type determining logic ([0066]-[0067] on pgs. 18-20, e.g., selection system 360 in FIG. 3, selection system 800 in FIG. 8) to determine whether a client device requesting a secure connection is a wired client device (e.g., wired access device 320 in FIG. 3) or a wireless client device (e.g., wireless access device 305 in FIG. 3). The apparatus also comprises logic to perform a wired authentication ([0136] on pg. 44, e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case SSL in FIG. 12, [0167] on pg. 52, block 1806 in FIG. 18, PKI module 2308 in FIG. 23) to establish the secure connection when it is determined that the requesting client device is the wired client device (e.g., wired access device 320 in FIG. 3). The apparatus also comprises logic to perform a wireless authentication ([0136] on pg. 44, e.g., blocks 1106 and 1108 in FIG. 11;

complete authentication for case WTLS in FIG. 12, [0163] on pg. 51, block 1706 in FIG. 17, WPKI module 2310 in FIG. 23) to establish the secure connection when it is determined that the requesting client device is the wireless client device (e.g., wireless access device 305 in FIG. 3). The apparatus also comprises logic to convert the SSL encrypted data to an unencrypted format (e.g., SSL conversion system 374 in FIG. 3, [0189] on pg. 59, SSL module 2304 in FIG. 23) and to convert the WTLS encrypted data to an unencrypted format (e.g., WTLS conversion system 372 in FIG. 3, [0190] on pg. 59, WTLS module 2306 in FIG. 23). The apparatus also comprises a second interface ([0073] on pg. 22, e.g., network interface 380 in FIG. 3; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to provide the data in the unencrypted formats to the server of the data center.

Independent claim 42 pertains to a method (see e.g., FIG. 4, [0079] on pg. 24, FIG. 12, [0139] pg. 45, etc.), according to a first embodiment of the invention. The method comprises receiving data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4, [0093] on pg. 29) (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4) within a data center (e.g., data center 150 in FIG. 1; data center 340 in FIG. 3, [0062]-[0065] on pgs. 17-18; data center 1316 in FIGs. 13, 14, 15, and 19) through a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) from at least one wired client device (e.g., wired access device 320 in FIG. 3) and at least one wireless client device (e.g., wireless access device 305 in FIG. 3) each requesting a secure connection with a server of the data center (e.g., server 390 in FIG. 3, [0073]-[0077] on pgs. 22-23; server 1314 in FIGs. 13, 14, 15, and 19). The method also comprises performing a wired authentication (e.g., blocks 1106 and 1108 in FIG. 11, [0136] on pg. 44; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, [0167] on pg. 52, PKI module 2308 in FIG. 23) to establish the secure connection with the wired client device. The method also comprises performing a wireless authentication (e.g., blocks 1106 and 1108 in FIG. 11, [0136] on pg. 44; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, [0163] on pg. 51, WPKI module 2310 in FIG. 23) to establish the secure connection with the wireless client device. The

method also comprises converting the data from an encrypted format to an unencrypted format (e.g., SSL conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23, [0189] on pg. 59; and e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23, [0190] on pg. 59). The method also comprises providing the data in the unencrypted format to the server of the data center through an interface (e.g., network interface 380 in FIG. 3, [0073] on pg. 22; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19).

Independent claim 50 pertains to an article comprising a machine-readable medium having stored thereon instructions that if executed cause a machine to perform operations (e.g., paragraph [0039]-[0040] on pg. 8 and original claim 26), according to a first embodiment of the invention. The operations comprise receiving first encrypted data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4, [0093] on pg. 29) through a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) from at least one wired client device (e.g., wired access device 320 in FIG. 3, [0061]-[0062] on pg. 17) and second encrypted data (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4, [0089] on pg. 28) through the public network from at least one wireless client device (e.g., wireless access device 305 in FIG. 3, [0060] on pg. 16) each requesting a secure connection with a server (e.g., server 390 in FIG. 3; server 1314 in FIGs. 13, 14, 15, and 19) within a data center (e.g., data center 150 in FIG. 1, [0044]-[0047] on pgs. 10-11; data center 340 in FIG. 3; data center 1316 in FIGs. 13, 14, 15, and 19). The operations also comprise performing a wired authentication (e.g., blocks 1106 and 1108 in FIG. 11, [0136] on pg. 44; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, [0167] on pg. 52, PKI module 2308 in FIG. 23) to establish the secure connection with the wired client device. The operations also comprise performing a wireless authentication (e.g., blocks 1106 and 1108 in FIG. 11, [0136] on pg. 44; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, [0163] pg. 51, WPKI module 2310 in FIG. 23) to establish the secure connection with the wireless client device. The operations also comprise converting the first encrypted data to a plain data format and converting the second encrypted data to a plain data format (e.g., SSL

conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23, [0189] on pg. 59; and e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23, [0190] on pg. 59). The operations also comprise providing the converted data in the plain data formats to the server through an interface (e.g., network interface 380 in FIG. 3, [0073] on pg. 22; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19). The machine-readable medium comprises one of a disk and a memory (paragraphs [0039]-[0040] on pg. 8).

Independent claim 56 pertains to an apparatus (e.g., security system 160 in FIG. 1; security system 345 in FIG. 3; security system 1312 in FIGs. 13, 14, 15, and 19; security system 2300 in FIG. 23), according to a first embodiment of the invention. The apparatus comprises a network interface (e.g., network interface 350 in FIG. 3, [0064]-[0066] on pgs. 18-19, interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to receive Secure Sockets Layer (SSL) data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4, [0093] on pg. 29) from a wired device through a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) and Wireless Transport Layer Security (WTLS) data (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4, [0089] on pg. 28) from a wireless device through a public network. The apparatus also comprises Public Key Infrastructure (PKI) logic (e.g., blocks 1106 and 1108 in FIG. 11, [0136] on pg. 44; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, [0167] on pg. 52, PKI module 2308 in FIG. 23) to establish a secure connection with the wired device. The apparatus also comprises Wireless Public Key Infrastructure (WPKI) logic (e.g., blocks 1106 and 1108 in FIG. 11, [0136] on pg. 44; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, [0163] on pg. 51, WPKI module 2310 in FIG. 23) to establish a secure connection with the wireless device. The apparatus also comprises SSL logic (e.g., SSL conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23, [0189] on pg. 59) to convert the SSL data to another format. The apparatus also comprises WTLS logic (e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23, [0190] on pg. 59) to convert the WTLS data to another format. The apparatus also comprises a second interface (e.g., network interface

380 in FIG. 3, [0073] on pg. 22; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to provide the data converted from the SSL and WTLS formats to a server (e.g., server 390 in FIG. 3, [0073]-[0077] on pgs. 22-23; server 1314 in FIGs. 13, 14, 15, and 19) over a private network.

Independent claim 59 pertains to a single network device (e.g., security system 160 in FIG. 1; security system 345 in FIG. 3, [0074]-[0078] on pgs. 22-24; security system 1312 in FIGs. 13, 14, 15, and 19; security system 2300 in FIG. 23), according to a first embodiment of the invention. The single network device is to be coupled within a data center (e.g., data center 150 in FIG. 1; data center 340 in FIG. 3, [0062]-[0065] on pgs. 17-18; data center 1316 in FIGs. 13, 14, 15, and 19) between a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) and a server (e.g., server 390 in FIG. 3, [0073]-[0077] on pgs. 22-23; server 1314 in FIGs. 13, 14, 15, and 19) of the data center. The single network device comprises a first interface (e.g., network interface 350 in FIG. 3, [0064]-[0066] on pgs. 18-19, interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to the public network, the first interface to receive first data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4, [0093] on pg. 29) that has been encrypted according to a wired encryption protocol from a wired device, and the first interface to receive second data (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4, [0089] on pg. 28) that has been encrypted according to a wireless encryption protocol from a wireless device. The single network device also comprises logic to perform a wired authentication (e.g., blocks 1106 and 1108 in FIG. 11, [0136] on pg. 44; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, PKI module 2308 in FIG. 23) with the wired device. The single network device also comprises logic to perform a wireless authentication (e.g., blocks 1106 and 1108 in FIG. 11, [0136] on pg. 44; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, WPKI module 2310 in FIG. 23) with the wireless device. The single network device also comprises logic to convert the first data to first unencrypted data (e.g., SSL conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23 [0189] on pg. 59) and to convert the second data to

second unencrypted data (e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23, [0190] on pg. 59). The single network device also comprises a second interface (e.g., network interface 380 in FIG. 3, [0073] on pg. 22; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to provide the first and second unencrypted data to the server of the data center.

CONCLUSION

Appellants respectfully petition for an extension of time should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee or any other required fee. Please charge any shortages and credit any overpayment to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 3/11/10

By Brent E. Vecchia

Brent E. Vecchia, Reg. No. 48,011
Tel.: (303) 740-1980 (Mountain Time)

1279 Oakmead Parkway
Sunnyvale, California 94085-4040